Release Notes

Secure Remote Access

SonicWALL SSL VPN 2.5 for SSL-VPN 200

Contents

Platform Compatibility

The SonicWALL SSL VPN 2.5 release is supported on the following platforms:

- **SonicWALL SSL VPN 200**

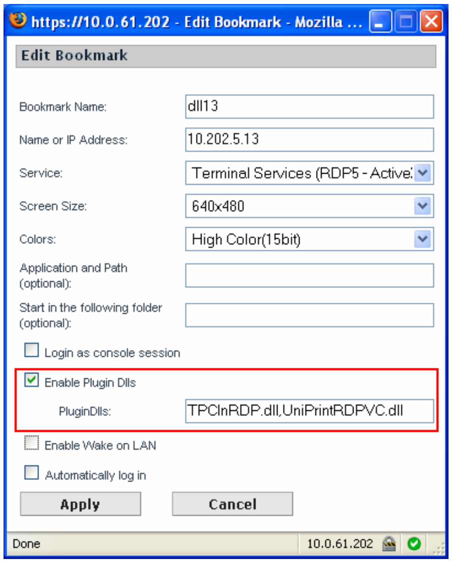
New Features

The following new features are supported on the SonicWALL SSL VPN 2.5 release:

- **NetExtender for Mac & Linux**: SSL VPN 2.5 has a NetExtender client that is compatible with MacOS and Linux systems. It uses a similar graphical layout and has many of the same basic features as the NetExtender client for Windows for ease of use.
  Mac Requirements:
  - Mac OS X 10.4+
  - Apple Java 1.4+ (can be installed/upgraded by going to Apple Menu > Software Update; should be pre-installed on OS X 10.4+)

  Linux Requirements:
  - i386-compatible distribution of Linux
  - Fedora Core and Ubuntu.
  - Sun Java 1.4+
- **NetExtender Windows Client Enhancements**: The NetExtender client for Windows from SSL VPN 2.5 comes with added features and improved functionality including a new log system and log viewer that supports flexible log formats, such as binary log files. The standalone log viewer can filter logs by time and log levels.
  Another new feature is the stand-alone client upgrade feature. The NetExtender client will automatically check for a newer version of the client at the SSL-VPN appliance and automatically upgrade. Older versions do not check for a newer version and must be upgraded manually to remain compatible with future features.
- **Portal Enhancements**: SSL VPN 2.5 features numerous enhancements to the Portal configuration capabilities including new management rules that can be set for HTTP, HTTPS, and Ping.
- **Per Bookmark Single Sign-On Credentials:** SSL VPN 2.5 supports custom Single Sign-On credentials for individual RDP and FTP bookmarks.
- **Reverse-Proxy Enhancements**:
  - URL/Port based policies
  - Variable response size
- **RDP Enhancements**: SSL VPN 2.5 supports the ‘Login as Console’ option, the ability to control the number of colors used in RDP sessions, the ‘Execute in Folder’ option, Plugin DLLs, and the Wake-on-LAN option. The Wake-on-LAN option can invoke multiple machines if their MAC addresses are separated by spaces.

- **Plugin DLLs**: The plugin DLLs feature allows for the use of certain third party programs such as print drivers, on a remote machine. This feature requires RDP Client Control version 5 or higher.



Edit Bookmark

Bookmark Name: dll13

Name or IP Address: 10.202.5.13

Service: Terminal Services (RDP5 - Active

Screen Size: 640x480

Colors: High Color(15bit)

Application and Path (optional):

Start in the following folder (optional):

□ Login as console session

☑ Enable Plugin Dlls

PluginDlls: TPClnRDP.dll,UniPrintRDPVC.dll

□ Enable Wake on LAN

□ Automatically log in

Client DLLs which need to be accessed by remote desktop or terminal service need to put in the Plugin DLLs field separated by commas. Make sure those DLLs are located in %SYSTEMROOT%\system32\ (i.e. C:\WINDOWS\system32\). If they are not in this directory, the user needs to manually copy those files to that location.

Troubleshooting Plugin DLLs:

If your system cannot get Plugin DLLs to work, please install our bundle version of MSRDP following these steps:

1. Go to http://sslvpn_server/msrdp.cab
2. Download msrdp.cab and save it in your local system (such as C:\tmp)
3. Extract the contents of the msrdp.cab file
4. Navigate the command line to the location in where you extracted the msrdp file, run this command to register it: “regsvr32 msrdp.ocx”
5. Restart your browser, it should now be able to access RDP-ActiveX bookmarks

If the above steps have been tried, and plugin DLLs still do not work, then try to un-register and re-register the RDP file by following these steps:

1. Run the command line at the msrdp location, un-register it by running “regsvr32 /u msrdp.ocx”
2. Restart your browser, and retry the RDP-ActiveX bookmark.
3. Register it again by running “regsvr32 msrdp.ocx” and repeat step 2.

Window XP (service pack 2) has a compatibility issue with remote desktop web connection. Please refer to the following link for more information: http://dev.remotenetworktechnology.com/ts/fixmsrdp.htm.
You can download the latest msrdp version from Microsoft from the following location:
http://www.microsoft.com/downloads/d...DisplayLang=en.

1. Download the tswebsetup.exe file from above link and install in your system,
2. Navigate to C:\Inetpub\wwwroot\TSWeb (the install location)
2. Run the command “regsvr /u msrdp.ocx” (to un-register the original)
3. Run the command “regsvr msrdp.ocx” (to register the new one).
4. Restart your browser and try the plugin DLL

Known Issues

This section contains a list of known issues in the SonicWALL SSL VPN 2.5 release.

- **64005**: **Symptom**: Importing appliance certificates can fail, instead redirecting the user to a blank page titled: NetExtender for Windows. **Condition**: Occurs when attempting to import certificate from the portal on Vista Ultimate when using IE7 browser.
  Workaround: To import certificates on Vista Ultimate, follow these steps:

  1. Right-click on Internet Explorer and select 'Run as Administrator.'
  2. Navigate to your site, on the warning page select to continue to the site
  3. Click on the Certificate Error in the address bar, and then view the certificate.
  4. Click the option to install the cert.
  5. When you're running the import cert wizard, choose the option to "place all certificates in the following store".
  6. Click Browse, then click to select 'Show physical locations'
  7. Scroll up in the list, expand Trusted Root Certification Authorities and select Local Computer.
  8. Click OK, then finish the import certificate wizard.
  9. Close IE and restart it as normal user.

- **64026**: **Symptom**: Importing appliance certificates can fail, instead redirecting the user to a blank page. **Condition**: Occurs when attempting to import certificate from the portal onto non-Windows clients and web browsers that do not support VBScript browsers.
- **63827**: **Symptom**: The appliance is unable to install an older firmware version. Attempting to do so results in the appliance becoming unresponsive. **Condition**: Occurs when downgrading from 2.5 to 2.1. **Workaround**: Make sure to boot the appliance with Factory Defaults when downgrading.
- **63965**: **Symptom**: Passwords cannot be changed. **Condition**: Occurs when credentials are updated and Active Directory is configured as an LDAP server. The new password will not be accepted at login, but the original one will still work.
- **64010**: **Symptom**: The client is able to access only one RDP session at a time. Connecting to more than one terminal using multiple RDP-Java bookmarks is not possible. **Condition**: Occurs when the Java client attempts to login to multiple RDP resources.
- **64077**: **Symptom**: The user is not informed that the portal inactivity timeout period has expired and the user has in fact been logged out. The browser will continue to display the portal until the user clicks on something, at which point the user will be redirected to a login screen. **Condition**: Occurs when the timeout period has expired.
- **64012**: **Symptom**: NetExtender does not show a warning when using incorrect credentials. Instead, it just keeps prompting for proxy authentication. **Condition**: Occurs when logging into a proxy server using incorrect credentials.
- **64011**: **Symptom**: NetExtender connects through the local connection if the proxy connection fails. **Condition**: Occurs when NetExtender is set to use an automatic configuration script for the proxy connection, and the script is incorrect (absent or badly formatted).
- **63967**: **Symptom**: Some web URL with embedded Chinese characters may not be reachable through bookmarks. Clicking the bookmark instead leads to the message “page cannot be found”. **Condition**: Occurs when trying to reach Chinese URLs using the Firefox browser.
- **63959**: **Symptom**: A user can still login even if he does not match the LDAP attribute requirements. **Condition**: Occurs when the user was once a correct user and has previously logged in. The user will remain able to login even if the requirements are updated in such a way that the user should no longer be able to.

- **63859**: **Symptom**: The NetExtender PPP Server’s IP address is not being set correctly. **Condition**: Occurs when attempting to set up a PPP server on a Vista system.
- **63851**: **Symptom**: Successful login attempts are being recorded twice in the logs with the same time stamp. **Condition**: Occurs when the user logs in as an administrator.
- **63830**: **Symptom**: Upgrading firmware can fail with the following error: "Error: Firmware Upload Failed - Memory allocation failed due to fragmentation. Please reboot the device and try again." **Condition**: Occurs when upgrading firmware on a SSL-VPN 200 appliance.

Resolved Issues

This section contains a list of resolved issues in the SonicWALL SSL VPN 2.5 release.

- **41804**: **Symptom**: Websites that use ISA-2022-JP characters (Japanese characters) do not display properly. Japanese characters appear garbled. **Condition**: Occurs when accessing the site through a VPN bookmark.
- **41801**: **Symptom**: Network objects with names in Japanese cannot be deleted. **Condition**: Occurs when using the trash icon to delete a network object that includes Japanese characters.
- **64078**: **Symptom**: NetExtender sessions seem to persist even after logging out from the portal. The connection remains until the user tries to access a remote resource, then it disconnects. **Condition**: Occurs when logging out from the portal.
- **63698**: **Symptom**: The Web browser goes down when multiple RDP-Java sessions are closed simultaneously. **Condition**: Occurs when closing an active RDP session in which two or more bookmarks were active.
- **64009**: **Symptom**: Warning dialog boxes keep popping up after logging out of the portal. **Condition**: Occurs when logging out from a portal in which “Enable ActiveX Web cache cleaner” is enabled. The cleaner attempts to delete cashed Web pages, which results in the looping warnings.
- **63991**: **Symptom**: Certificates cannot be imported as a zipped directory. Their status is displayed as ‘pending’ but they remain blank and cannot be deleted afterwards. C**ondition**: Occurs when importing a .zip file containing a CSR directory that in turn has a server.crt and a server.key file.
- **63695**: **Symptom**: The Active X client does not support the use of custom port number for RDP connections. The client will return the following error message: “Because of a portal error, this session will be disconnected. Please try connecting to the remote computer again.” **Condition**: Occurs when using a bookmark to a RDP resource with a customized port number.
- **63482: Symptom:** Login credentials for administrator shares are not cached by the file shares in HTML. When accessing administrator shares for the second time without logging out from the portal, the application should not ask for credentials again. **Condition:** Occurs when accessing admin shares for the second time without logging out from the portal.
- **50779: Symptom:** When using single-sign-on to access the file share bookmark as an AD/NT, login fails if the “Domain Name” field is used. If the “Domain Name” field does not match the AD/NT domain name, single-sign-on will not work. **Condition:** Occurs when accessing a file share bookmark using the “Domain Name” field.
- **47448: Symptom:** Downloading, renaming, and deleting GMS reports fails. **Condition:** Occurs when users create reports with more than the allowed maximum characters in the file name. File name limit is 70 characters for Unix servers, or 90 characters for MS-Dos severs.
- **41653**: **Symptom**: IP network cannot be deleted from a network object. **Condition**: Occurs when a network object is modified to remove an IP network.

Upgrading SonicWALL SSL VPN Software Procedures

The following procedures are for upgrading an existing SonicWALL SSL VPN image to a newer version.

- OBTAINING THE LATEST SONICWALL SSL VPN IMAGE VERSION
- EXPORTING A COPY OF YOUR CONFIGURATION SETTINGS
- UPLOADING A NEW SONICWALL SSL VPN IMAGE
- RESETTING THE SONICWALL SSL VPN 200 USING SAFEMODE

Obtaining the Latest SonicWALL SSL VPN Image Version

1. To obtain a new SonicWALL SSL VPN image file for your SonicWALL security appliance, connect to your mysonicwall.com account at <http://www.mysonicwall.com>.

   Note: *If you have already registered your SonicWALL SSL VPN appliance, and you selected* ***Notify me when new firmware is available*** *on the* ***System > Settings*** *page, you are automatically notified of any updates available for your model.*

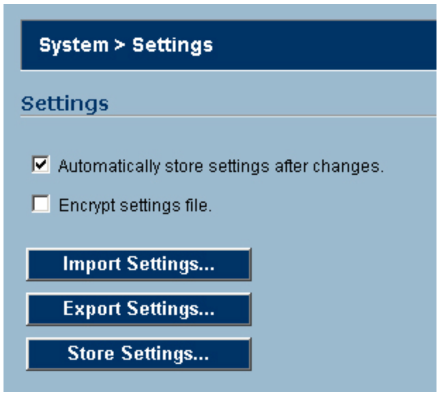
2. Copy the new SonicWALL SSL VPN image file to a directory on your management station.

Exporting a Copy of Your Configuration Settings

Before beginning the update process, export a copy of your SonicWALL SSL VPN appliance configuration settings to your local machine. The Export Settings feature saves a copy of your current configuration settings on your SonicWALL SSL VPN appliance, protecting all your existing settings in the event it becomes necessary to return to a previous configuration state.

Perform the following procedures to save a copy of your configuration settings and export them to a file on your local management station:

1. Click the **Export Settings . . .** button on the **System > Settings** page and save the settings file to your local machine. The default settings file is named *sslvpnSettings.zip*.



System > Settings

Settings

☑ Automatically store settings after changes.

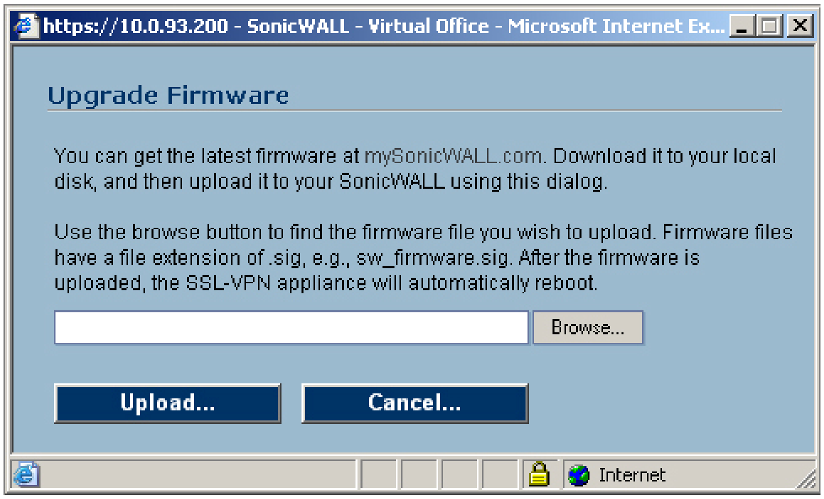
☐ Encrypt settings file.

Tip: To more easily restore settings in the future, rename the .zip file to include the version of the SonicWALL SSL VPN image from which you are exporting the settings.

Uploading a New SonicWALL SSL VPN Image

Note: *SonicWALL SSL VPN appliances do not support downgrading an image and using the configuration settings file from a higher version. If you are downgrading to a previous version of a SonicWALL SSL VPN image, you must select* ***Uploaded Firmware with Factory Defaults – New!*** *. You can then import a settings file previously saved from the downgrade version or reconfigure manually.*

1. Download the SonicWALL SSL VPN image file from www.mysonicwall.com and save it to a location on your local computer.
2. Select **Upload New Firmware** from the **System > Settings** page. Browse to the location where you saved the SonicWALL SSL VPN image file, select the file, and click the **Upload** button. The upload process can take up to one minute.



https://10.0.93.200 - SonicWALL - Virtual Office - Microsoft Internet Ex...

Upgrade Firmware

You can get the latest firmware at mySonicWALL.com. Download it to your local disk, and then upload it to your SonicWALL using this dialog.

Use the browse button to find the firmware file you wish to upload. Firmware files have a file extension of .sig, e.g., sw_firmware.sig. After the firmware is uploaded, the SSL-VPN appliance will automatically reboot.

3. When the upload is complete, you are ready to reboot your SonicWALL SSL VPN appliance with the new SonicWALL SSL VPN image. You can either reboot the SonicWALL SSL VPN appliance with the current settings or with the factory default settings:

   a. To reboot the image with current preference, click the boot icon for the following entry: **Uploaded Firmware – New!**

   b. To reboot the image with factory default settings, click the boot icon for the following entry: **Uploaded Firmware with Factory Defaults – New!**

   Note: *Be sure to save a backup of your current configuration settings to your local machine before rebooting the SonicWALL SSL VPN appliance with factory default settings, as described in the previous "Saving a Backup Copy of Your Configuration Settings" section.*

4. A warning message dialog is displayed saying **Are you sure you wish to boot this firmware? Click OK to proceed**. After clicking OK, do not power off the device while the image is being uploaded to the flash memory.
5. After successfully uploading the image to your SonicWALL SSL VPN appliance, the login screen is displayed. The updated image information is displayed on the **System > Settings** page.

Resetting the SonicWALL SSL VPN 200 Using SafeMode

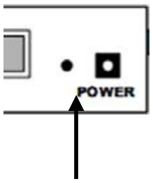
If you are unable to connect to the SonicWALL security appliance’s management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

To reset the SonicWALL security appliance, perform the following steps:

1. Connect your management station to a LAN port on the SonicWALL security appliance and configure your management station IP address with an address on the 192.168.200.0/24 subnet, such as 192.168.200.20.

   Note: *The SonicWALL security appliance can also respond to the last configured LAN IP address in SafeMode. This is useful for remote management recovery or hands off recovery in a datacenter.*

2. Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the security appliance for five to ten seconds. The reset button is in a small hole next to the power supply.

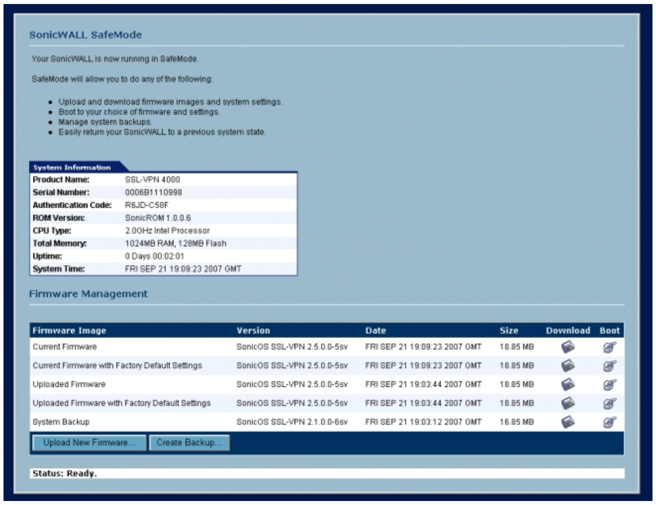
   

   Reset Button – SSL VPN

   Tip: *If this procedure does not work while the power is on, turn the unit off and on while holding the reset button until the Test light starts blinking.*

   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

3. Connect to the management interface: Point the Web browser on your management station to **http://192.168.200.1**. The SafeMode management interface displays.

   SonicWALL SafeMode

   Your SonicWALL is now running in SafeMode.

   SafeMode will allow you to do any of the following:

   - Upload and download firmware images and system settings.
   - Boot to your choice of firmware and settings.
   - Manage system backups.
   - Easily return your SonicWALL to a previous system state.

System Information	
Product Name:	SSL-VPN 4000
Serial Number:	0006B1110998
Authentication Code:	R6JD-C58F
ROM Version:	SonicROM 1.0.0.6
CPU Type:	2.0GHz Intel Processor
Total Memory:	1024MB RAM, 128MB Flash
Uptime:	0 Days 00:02:01
System Time:	FRI SEP 21 19:09:23 2007 GMT

   Firmware Management

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS SSL-VPN 2.5.0.0-5sv	FRI SEP 21 19:09:23 2007 GMT	18.85 MB		
Current Firmware with Factory Default Settings	SonicOS SSL-VPN 2.5.0.0-5sv	FRI SEP 21 19:09:23 2007 GMT	18.85 MB		
Uploaded Firmware	SonicOS SSL-VPN 2.5.0.0-5sv	FRI SEP 21 19:03:44 2007 GMT	18.85 MB		
Uploaded Firmware with Factory Default Settings	SonicOS SSL-VPN 2.5.0.0-5sv	FRI SEP 21 19:03:44 2007 GMT	18.85 MB		
System Backup	SonicOS SSL-VPN 2.1.0.0-6sv	FRI SEP 21 19:03:12 2007 GMT	16.85 MB		

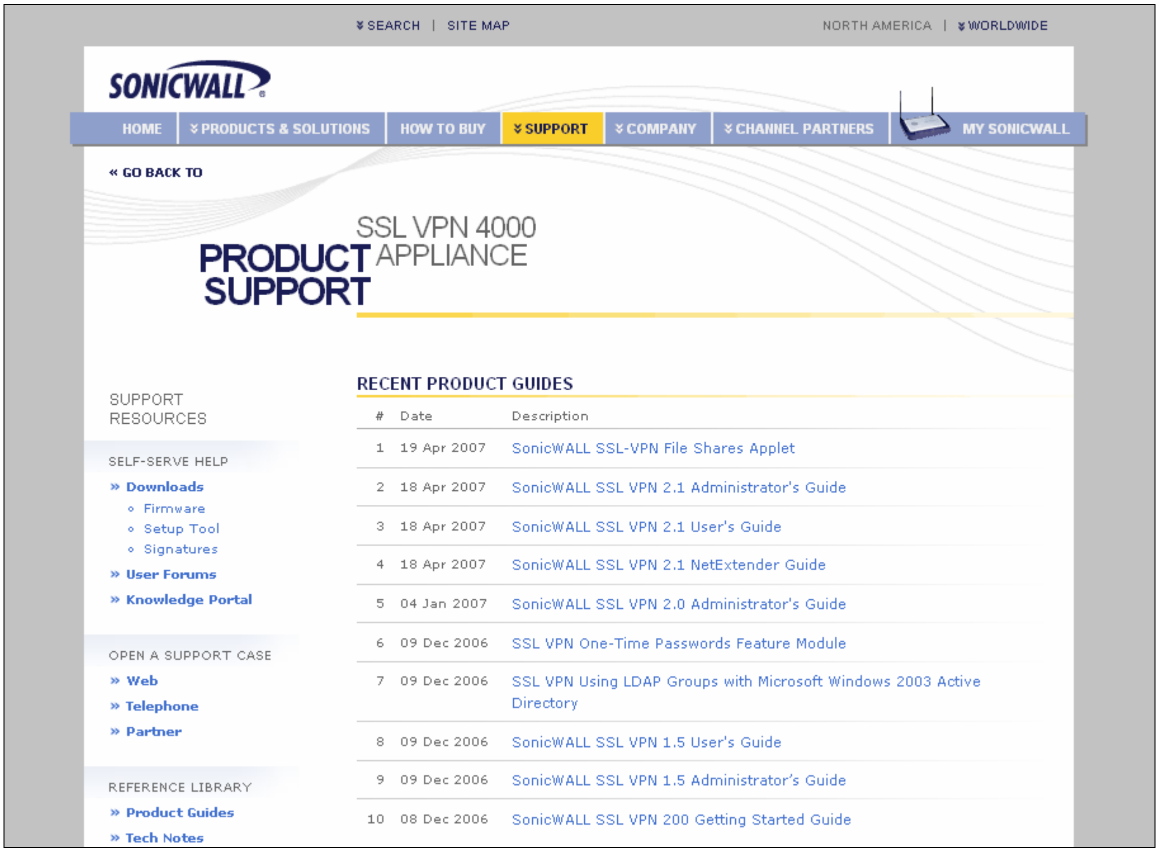
   Status: Ready.

4. Try rebooting the SonicWALL security appliance with your current settings. Click the boot icon in the same line with **Current Firmware**.

After the SonicWALL security appliance has rebooted, try to open the management interface again. If you still cannot open the management interface, use the reset button to restart the appliance in SafeMode again. In SafeMode, restart the SonicOS SSL VPN image with the factory default settings. Click the boot icon in the same line with Current Firmware with Factory Default Settings**.**

Related Technical Documentation

This section contains a list of technical documentation available on the SonicWALL Technical Documentation Online Library located at:
http://www.sonicwall.com/support/documentation.html



PRODUCT SUPPORT SSL VPN 4000 APPLIANCE

RECENT PRODUCT GUIDES

#	Date	Description
1	19 Apr 2007	SonicWALL SSL-VPN File Shares Applet
2	18 Apr 2007	SonicWALL SSL VPN 2.1 Administrator's Guide
3	18 Apr 2007	SonicWALL SSL VPN 2.1 User's Guide
4	18 Apr 2007	SonicWALL SSL VPN 2.1 NetExtender Guide
5	04 Jan 2007	SonicWALL SSL VPN 2.0 Administrator's Guide
6	09 Dec 2006	SSL VPN One-Time Passwords Feature Module
7	09 Dec 2006	SSL VPN Using LDAP Groups with Microsoft Windows 2003 Active Directory
8	09 Dec 2006	SonicWALL SSL VPN 1.5 User's Guide
9	09 Dec 2006	SonicWALL SSL VPN 1.5 Administrator's Guide
10	08 Dec 2006	SonicWALL SSL VPN 200 Getting Started Guide

The SonicWALL SSL VPN 200 appliances include the following reference guides:

- *SonicWALL SSL VPN 200 Getting Started Guide*
- *SonicOS SSL VPN 2.1 Administrator's Guide*
- *SonicOS SSL VPN 2.1 User's Guide*
- *SonicWALL Secure Wireless Integrated Solutions Guide*
- *Advanced Deployment Technotes*

Last updated: 1/31/2008